In Paragraphs 1 – 6 of the Office Action, claims 12 and 27 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen, U.S. Patent No. 6,032,150 ("Nguyen") in view of Andersen, U.S. Patent No. 5,999,941 ("Andersen").

Distinctions between Claimed Invention and U.S. Patent No. 6,032,150 to Nguyen in view of U.S. Patent No. 5,999,941 to Andersen

Independent claim 12 recites a combination including:

receiving from said software application via said network a request for information stored in a restricted access storage area of a server and

thereafter providing said information to said software application via said network while said associated password is valid.

Similarly, independent claim 27 recites a combination including:

a restricted-access storage area and

provide said information to said software application via said network while said associated password is valid.

Nguyen was discussed in the previous response. The Examiner did not repeat the anticipation rejection of the previous Office Action, and thus apparently agreed with applicants' characterization of Nguyen. Nguyen describes a method and system for protecting information such as graphical elements within a web document. Nguyen uses program applets, which are created when a user tries to access the protected information, to control access to the protected information. (Nguyen / col. 1, lines 55 – 67; col. 3, lines 12 – 30; claims 1, 8 and 15) Each applet includes a unique ID, which a server associates with one or more access conditions. When the applet executes to present protected information, it contacts the server for permission to do so. (Nguyen / col. 3, lines 31 – 39; claims 6, 13 and 19).

In contrast to the present invention in which the protected information resides on the server, the protected information of Nguyen is generated by the applet. Specifically, at col. 3, line 31 Nguyen states "*The program applet 124 is disposed to execute at the web client 110 and to present the graphical element 123 in further detail (or other further information) to the user at the web client 110.*" Additionally, claims 1, 8 and 15 of Nguyen recite "*said program applet being disposed to present said further information only upon selected conditions.*" Nguyen does not show protected information stored in a restricted-access storage area of a server, which is a feature of the present invention. (See, for example, original specification / page 11, lines 20 and 21; element 68 of FIG. 6 and FIG. 7; claim 27).

Anderson fails to correct the deficiencies of Nguyen. Andersen describes a web-based client application that uses a JAVA applet to send queries from a client computer to a database management system running on a server computer, and to receive query results embedded within HTML documents. Andersen describes (i) passing a database query embedded within a URL from the client computer to an active server page located on the server computer, (ii) creating an HTML page including the query results on the server computer, and (iii) delivering the HTML page to the client computer for processing and display. A script for the active server page performs the actual interfacing with the database management system itself.

In Paragraph 5 of the Office Action, the Examiner has indicated that Andersen discloses a software application that requests information stored in a storage area of a server. Moreover, in Paragraph 6 of the Office Action, the Examiner has indicated that Andersen recognizes the problem that giving JAVA applets free access on the network can give rise to a number of serious administrative and security problems.

Applicants respectfully submit that, in distinction from the present invention, Andersen does not disclose access of protected information in a storage area of a server.

Moreover, the administrative and security problems referred to by Andersen at col. 1, lines 45 – 47) refer to damage the applet can do to the client computer, similar to damage caused by computer viruses. Specifically, at col. 1, lines 47 – 54, Andersen recites "*If the applet was able to have free access to the full range of operating system calls accessed by application programs, then a web browser could inadvertently download from the Internet a capricious program that ... damages or destroys the client computer's file system and the content of the client computer's files ...*"

In fact, a feature of Andersen is that it specifically overcomes security issues by avoiding them. Thus, one of the prior art methods that Andersen overcomes is the JDBC-ODBC bridge, that "*has the drawback that ... the applet must adhere to a number of security requirements.*" (Andersen / col. 2, lines 49 – 59). Thus, Andersen favors use of HTML pages, since "*applets have relatively free access to HTML pages unconstrained by security requirements.*" (Andersen / col. 2, lines 59 – 61) Similarly, at col. 3, lines 48 – 50, Andersen recites "*This technique avoids the general security issues involved in accessing resources from a JAVA applet*"; at col. 4, lines 11 – 13, Andersen recites "*The security problems that would arise from an attempt to directly connect to the database management system from within a JAVA applet are thus completely avoided ...*"; and at col. 4, lines 65 – 67 Andersen recites "*There are no security issues, since the applet makes no attempt to access resources other than HTML pages via normal URL-specified access.*"

As such, applicants respectfully submit that at least the limitations in claim 12 of:

"*receiving from said software application via said network a request for information stored in a restricted access storage area*" and

"*thereafter providing said information to said software application via said network while said associated password is valid*"

are neither shown nor suggested in Nguyen or Andersen, taken alone or in combination.

Similarly, applicants respectfully submit that at least the limitations in claim 27 of:

"*a restricted-access storage area*" and

"*provide said information to said software application via said network while said associated password is valid*"

are neither shown nor suggested in Nguyen or Andersen, taken alone or in combination.

The other pending claims depend from one of independent claims 12 and 27 and are patentably distinct from the cited references for at least the reasons discussed above.

For the foregoing reasons, applicants respectfully submit that the claims are in condition for allowance.

Respectfully Submitted,
DANIEL SCHREIBER AND DAVID GUEDALIAH

Dated: 8/8/02

By: _____
Greg T. Sueoka, Reg. No.: 33,800
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306
Tel: (650) 858-7194
Fax: (650) 494-1417